SPECIALE

SUPPLEMENTO AL
N. 2/88 DI ULTIMOBYTE
LIRE 15.000

# Ultimobyte

FLOPPIRIVISTA PER PC COMPATIBILI



**2 PROGRAMMI ANTISABOTAGGIO**

*SICUREZZA E CIFRATURA DEI DATI*

**COME SI COMBATTONO I VIRUS**

*RESUSCITARE FILES CANCELLATI*

Spediz. Abbonamento Postale - Gruppo III/70

SPECIALE
Ultimobyte
Supplemento al n. 2/88
di Ultimobyte
Direttore responsabile
Adalberto Fontana
Hanno collaborato
a Speciale Ultimobyte
Sigfrido Ghidini
Lucia Giordano
Mauro Giudici
Paolo Maier
Verdesoto
Autorizzazione
del Tribunale di Milano
N. 373 del 20-7-1985
Distribuzione per l'Italia
Messaggerie Periodici S.p.A.
Viale Famagosta, 75
20142 Milano
Tel. 02/8467545
Aderente A.D.N.
Stampa
Garzanti Editore S.p.A.
Via Senato, 25
20121 Milano
Duplicazione floppy
Datamatic S.p.A.
Pubblicità e Abbonamenti
Ultimobyte Editrice S.r.l.
Via A. Manuzio, 15
20124 Milano
Tel. 02/6597693
Pubblicità inferiore al 70%
Ultimobyte - Floppirivista per
PC compatibili
è una pubblicazione
mensile della
Ultimobyte Editrice S.r.l.
Via A. Manuzio, 15
20124 Milano
Una copia
Speciale Ultimobyte L. 15.000
Arretrati L. 20.000
Abbonamento annuo
(11 numeri) L. 140.000

# Come leggere Ultimobyte

## 1

**Configurazioni con 2 drives a floppy**

- Disco sistema in A e disco Ultimobyte in B
- A>B:[ENTER]
- B>RIVISTA [ENTER]

## 2

**Configurazioni con disco rigido**

- Boot da disco rigido
- Disco Ultimobyte in A
- C>A:[ENTER]
- A>RIVISTA [ENTER].

***Compare subito la copertina e, dopo breve intervallo musicale, il Sommario in sovraimpressione.***

## 3

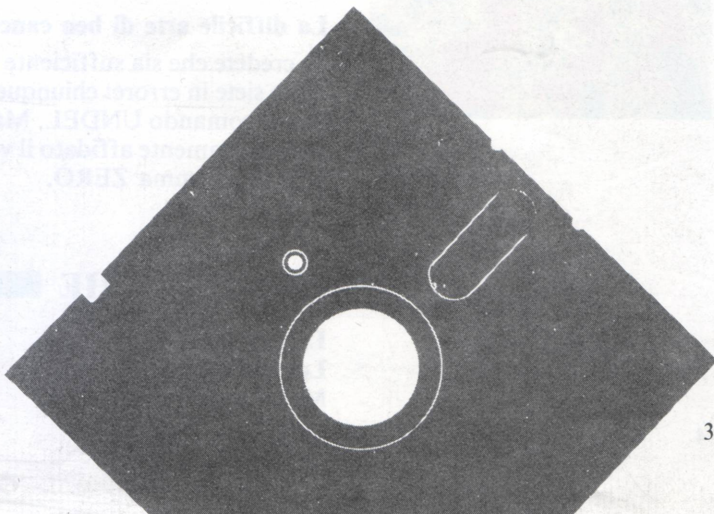
Usate il tasto **[ESC]** per selezionare una delle due modalità: "diretta" o "comando". Indi, con la **barra spaziatrice** scegliete l'articolo da leggere (modalità diretta) o il comando da eseguire (SCORRI per vedere uno degli abstract del Sommario, AUTO per leggere gli abstract in sequenza, ESCI per abbandonare la rivista). Convalidate la scelta premendo [ENTER]. La sequenza degli abstract in AUTO può essere interrotta con [ESC], che causa la ricomparsa del Sommario, o con [BACKSPACE], con cui si torna alla lettura dell'articolo.

## 4

Con il comando ESCI (vedi punto precedente) o con la sequenza [SHIFT] + [F9], sempre utilizzabile, si abbandona definitivamente la rivista. Con il tasto [F1] si può richiamare il DOS da un punto qualsiasi di ogni articolo (non da un abstract): per tornare all'articolo basta battere EXIT seguito da [ENTER] al prompt.

## 5

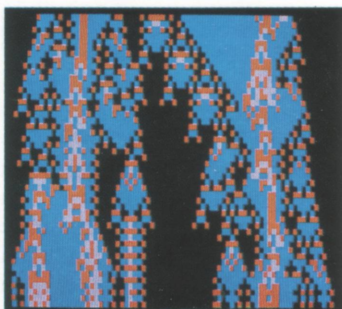
Con 128K di memoria può capitare che non riusciate a lanciare un programma direttamente dalla rivista (tasti [F1] e [F2]), causa il poco spazio a disposizione. In questi casi dovete copiare il programma su un vostro disco e lanciarlo normalmente.Con monitor B/W otterrete una maggiore leggibilità abbandonando la rivista (SHIFT + F9) ed eseguendo al prompt **BW80.** Rilanciate quindi RIVISTA.





# SOMMARIO

Speciale Ultimobyte
Supplemento al N. 2/88 di Ultimobyte



## VITA VISSUTA



Sia esso stato inventato per gioco, per sfregio, per sabotaggio o per competizione, il virus della pallina si rivela più imbecille che astuto. Paolo Maier vi spiega come agisce e come si può sconfiggere questa particolare categoria di virus.

## DIFESE PASSIVE

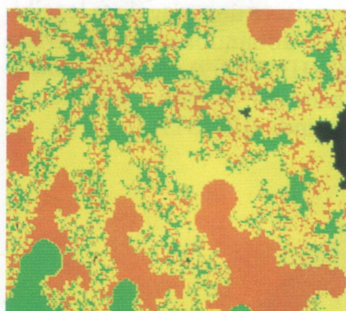


Dagli Stati Uniti ci pervengono due programmi, BOMBSQAD e CHK4BOMB, che servono per intercettare ed eventualmente neutralizzare i comportamenti potenzialmente pericolosi riscontrati nel programma che state per eseguire. Due fedeli cani antisabotaggio che mordono solo a comando, ma abbaiano sempre abbastanza forte da richiamare la vostra attenzione.

## DIFESE ATTIVE



Cifrare un file di dati vuol dire renderlo praticamente inaccessibile a chi non sia in possesso della chiave di lettura. Questa semplice arma di difesa può risultare preziosa in più di una circostanza. Senza contare il risparmio sulla bolletta del telefono.



## IN PROFONDITÀ



Se credete che sia sufficiente la Delete per cancellare un file dal disco siete in errore: chiunque può resuscitarlo usando, ad esempio, il comando UNDEL. Ma il miracolo risulta inutile se avete preventivamente affidato il vostro file alle vigorose cure del nostro programma ZERO.

## LE RUBRICHE

# LA DIRECTORY

**In questo Speciale Ultimobyte abbiamo conservato la consueta struttura di Ultimobyte, ma non ci è parso utile mantenere il Banco di Prova. Ecco di seguito l'elenco commentato dei files che trovate sul disco e che potete copiare e usare a vostro piacimento.**

- **DEVIRUS.COM** Il programma in formato eseguibile che serve ad eliminare il virus della pallina

- **CHK4BOMB.EXE** Il programma in formato eseguibile che esamina un file e fornisce una diagnosi sulle attività potenzialmente pericolose che dovesse rilevare
- **BOMBSQAD.COM** Il programma in formato eseguibile che intercetta tutte le chiamate al BIOS e dà la possibilità di intervenire a bloccare quelle potenzialmente pericolose

- **ENCRYPT.EXE** Il programma in formato eseguibile che serve a cifrare e a decifrare un testo in base ad una chiave
- **COMPRESS.EXE** Il programma in formato eseguibile che serve a comprimere un file di testo

- **UNDEL.COM** Il programma in formato eseguibile che permette di recuperare un file cancellato con DEL
- **ZERO.COM** Programma in formato eseguibile che azzera un file prima di cancellarlo
- **ZERO1.EXE** Eseguibile di ZERO1.BAS
- **ZERO1.BAS** Programma in sorgente Basic che azzera un file prima di cancellarlo. Si lancia da BASICA o GWBASIC

- **NEWYORK.BAS** Sorgente Basic dell'avventura "Morte a New York", pubblicata su Ultimobyte N. 1/88
- **BUONO.BAT** File Batch che fa una TYPE di SOLUZ1 e fornisce una delle possibili soluzioni dell'avventura
- **CATTIVO.BAT** File Batch che fa una TYPE di SOLUZ2 e fornisce una delle possibili soluzioni dell'avventura

# Indice del Volume I Anno 1987

# Al mio lettore

*Milano, 22 febbraio 1988*

*Caro lettore,*

*Ti avevo promesso, nel lontano gennaio del 1987, tanti programmi e pochi editoriali. Da allora non ho più avuto occasione di rivolgermi a te, eppure spesso ho sentito l'esigenza perlomeno di ringraziarti del successo che hai decretato alla nostra pubblicazione e di giustificare il ritardo con il quale siamo fino ad ora usciti in edicola. Lo faccio adesso e ne approfitto anche per formulare la nuova promessa, quella del 1988: maggiore puntualità nell'appuntamento mensile con le edicole e un paio di numeri speciali, dedicati ad argomenti di attualità oppure a singoli programmi di particolare interesse e livello qualitativo.*

*Questa edizione straordinaria di Ultimobyte è stata pensata e realizzata nello spazio di qualche giorno e ho deciso di mandarla in stampa senza molto curare le rifiniture e privilegiando gli aspetti pratici rispetto a quelli cosmetici. Troppo importante mi è sembrato il fattore tempo, soprattutto dopo aver dovuto vittoriosamente combattere contro il famigerato virus della pallina e dopo aver letto sullo Herald Tribune di lunedì 1 febbraio la dichiarazione dello specialista in sicurezza Dennis Steinaur, secondo il quale «quest'anno ci sarà una gara tra i creatori di virus: vince chi concepisce quello più forte. Siamo tutti vulnerabili.».*

*Quello che in qualche maniera mi conforta è l'imbecillità del creatore di virus, che in molti casi agisce solo per gioco o per competizione, senza poter sfruttare praticamente la sua mostruosa creatura. Auspico e ritengo inevitabile che lo sport ipotizzato da Steinaur si trasformi presto in una gara tra creatori di virus e creatori di antidoti, dove tifo spudoratamente per questi ultimi, disposto a correre il rischio di avere a che fare con una nuova categoria di pentiti.*

*Nonostante che Maurizio Costanzo abbia a più riprese sostenuto la ininterrotta pregnanza della mamma degli imbecilli, personalmente ritengo che imbecilli si diventa, ma fortunatamente il processo non sembra irreversibile. Attendo fiducioso smentite e conferme.*

***Adalberto Fontana***

MEA CULPA

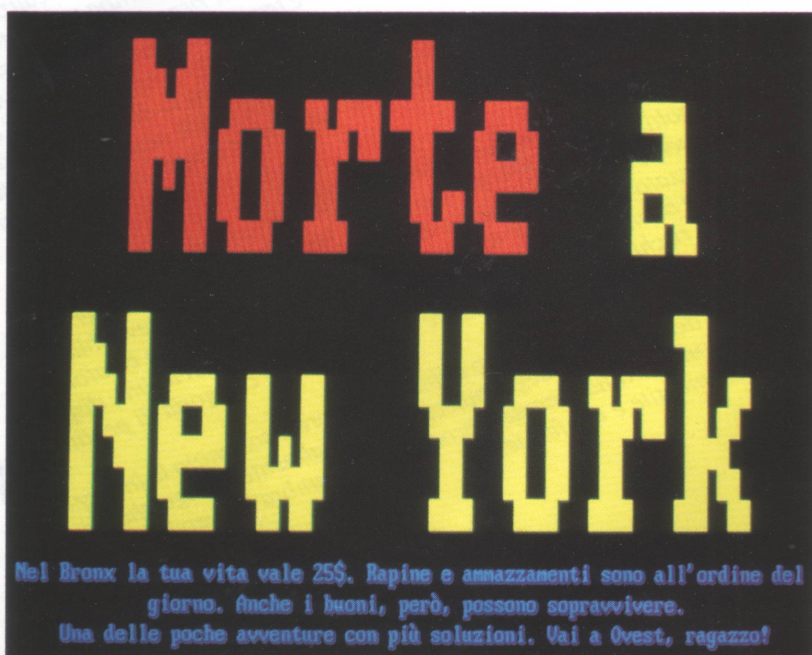
# Biglietto di sola andata

Alcuni lettori, evidentemente patiti di avventure, ci hanno fatto rilevare che Morte a New York, pubblicata sul N. 1/88 di Ultimobyte, da un certo momento in poi torna sempre allo stesso punto. Fatte le opportune verifiche, abbiamo potuto assodare che il comportamento anomalo si ritrova solo nella versione compilata del programma, mentre la versione interpretata funziona benissimo. Evidentemente abbiamo apportato alcune variazioni in fase di compilazione, che hanno trasformato l'avventura in un cul di sacco.

Siamo certi di fare cosa gradita a questi e a tutti gli altri lettori semplicemente curiosi pubblicando il sorgente di Morte a New York, insieme con due soluzioni, una per i buoni e l'altra per i malvagi.

Il file interessato si chiama NEWYORK.BAS e si lancia da Basic (BASICA o GWBASIC). Potete leggere le soluzioni battendo BUONO o CATTIVO, a seconda delle vostre inclinazioni: questi ultimi due files sono dei semplicissimi Batch che si limitano ad eseguire la TYPE rispettivamente di SOLUZ1 e SOLUZ2.

Crediamo che questo sia meglio di tante scuse, che comunque porgiamo ai lettori.





# Imbecilli si diventa

**Il virus della pallina è stato definito di volta in volta astuto, benigno e burlone. A noi pare più che altro imbecille**

Da qualche mese nei salotti buoni dell'informatica italiana l'argomento principe, ossia l'intelligenza artificiale, sembra sia stato momentaneamente messo in disparte in favore del nuovo arrivato, il virus del computer, che unisce a suggestioni apocalittiche il fascino morboso del serpente velenoso e il senso della sfida. Anche la grande stampa ha fiutato con straordinario tempismo la notizia "buona" e non si è lasciata sfuggire l'occasione per tornare a più riprese sul tema, che ha il pregio di interessare non solo le svariate centinaia di migliaia di potenziali vittime, ma anche, quale fenomeno di costume, la ben più consistente categoria dei semplici osservatori delle cose terrene.

A ben guardare, l'accento è stato prevalentemente posto sugli effetti nefasti derivanti dalla presenza di questi virus nel computer, vale a dire la distruzione dei dati e dei programmi registrati sui supporti magnetici, ma poco o nulla ci risulta essere stato fatto per la diffusione di conoscenze più specifiche, quali i modi di contagio e, soprattutto, i sistemi che permettono di intercettare, combattere e spesso prevalere sui fastidiosi e indesiderati ospiti. Questo nostro contributo deriva da esperimenti diretti compiuti in presenza del famigerato virus della pallina, che pare affliggere gli ambienti universitari di mezza Italia e che si materializza, quando casualmente decide di farlo, con una specie di beffarda palletta vagante per lo schermo.

La pallina, come vedremo tra breve, è un virus un po' imbecille, che non è stato creato propriamente da un mago del bit, ma che, comunque, può fornire parecchie indicazioni utili ad affrontare tutti i virus che appartengono a questa stessa categoria. Imbecille non vuol dire innocuo, anzi siamo pressoché certi che la pallina può procurare danni, tipicamente la distruzione dei files, al termine di un periodo di gestazione assai mutevole nella durata. Altri e ben diversamente attrezzati sono i virus tanto temuti dai dipartimenti della difesa delle superpotenze, con i problemi di sicurezza che si possono bene immaginare, oppure dalle multinazionali alle prese con non meno importanti questioni inerenti la definizione delle strategie aziendali.

Dal Politecnico di Torino alla Bocconi di Milano, la pallina semina comunque il panico tra gli studenti universitari alle prese con appelli di laurea e termini di consegna delle tesi, per la cui battitura vengono generalmente usati i PC messi a disposizione dalle stesse università. Volentieri accogliamo e giriamo a chi di dovere l'appello (non di laurea) che ci giunge da più parti: signori docenti, che cosa ne direste di applicare criteri più elastici — sui tempi, non certo sulle valutazioni di merito — almeno fino a quando il fenomeno non si sarà stabilizzato?

## Armiamoci e partiamo

**C'è virus e virus.** I virus di cui ci occupiamo in questo articolo possiedono tutti un paio di caratteristiche comuni che li fanno appartenere allo stesso ceppo:

- sono attivati da un richiamo normalmente posto nella traccia zero del disco, una di quelle riservate al sitema operativo.

Questa traccia viene scritta dal comando FORMAT (o SYS) ed è identica per tutti i dischi preparati con la stessa versione di Dos. Le Figure 1 e 2 mostrano il contenuto del primo settore della traccia zero rispettivamente in assenza e in presenza di virus.

- si propagano SOLO se il disco su cui risiedono è un disco di boot, ossia predisposto per far partire il computer. Infatti, per definizione, non possono caricare in memoria se stessi addirittura PRIMA del sistema operativo quando il boot venga effettuato da un disco non infetto. Naturalmente, la propagazione del virus non può avvenire neppure da un disco di boot infetto su dischi che abbiano l'etichetta di protezione contro operazioni di scrittura.

A questo punto le opinioni divergono. Secondo alcuni un disco infetto, ma non utilizzabile per il boot perché non contiene i due files nascosti (IBMBIO.COM e IBMDOS.COM oppure IO.SYS e MSDOS.SYS a seconda che si tratti di PC o di MS-DOS) e l'interprete dei comandi (COMMAND.COM) diviene innocuo dato che il virus non riesce mai ad attivarsi. Noi siamo invece del parere che in queste condizioni il virus NON si propaga, ma PUO' combinare danni limitatamente al disco su cui risiede. Assodato dunque che il contagio si propaga unicamente da UN DISCO DI BOOT INFETTO, vediamo ora quali sono i metodi per rilevare l'infezione e indichiamo alcuni antidoti.

**La grande caccia.** Il primo ovvio consiglio che possiamo darvi è quello di non fare MAI il boot da un disco di cui non conoscete la provenienza; come secondo provvedimento sarebbe utile, anche se non indispensabile, disporre di strumenti (Norton Utilities e Pctools solo per citare i più noti) che consentono un esame visivo della traccia zero, a meno che non sappiate utilizzare il DEBUG del Dos. Con uno di questi strumenti, infatti, sarebbe facile andare alla ricerca in traccia zero della parola PSQR, che non è l'anagramma di SPQR, bensì rivela la presenza del corpo estraneo, ovvero di una routine in linguaggio assembler che non dovrebbe proprio esserci e che con ogni probabilità è stata messa lì da qualche malintenzionato.

Tutto ciò serve però solo ai virus-killer professionisti, ma che cosa possono fare gli utenti "normali" del PC, che di Norton e Pctools non hanno mai sentito parlare e che sconoscono l'esistenza stessa di DEBUG? Abbiamo sperimentato diversi metodi che hanno tutti come scopo quello di riportare la traccia zero del disco infetto allo stato in cui era prima che qualcuno introducesse il maledetto PSQR.

È fondamentale che disponiate di una copia del sistema operativo sicuramente sana. Indipendentemente dalla vostra configurazione hardware dovreste avere conservato il disco originale del Dos consegnatovi al momento dell'acquisto del computer ed è proprio questo disco che vi consigliamo di usare. Di seguito diamo la sequenza delle operazioni da effettuare per la decontaminazione e ribadiamo che si tratta di nostri esperimenti, i quali fino ad ora hanno dato risultati positivi.

Caso A. *Siete certi che il vostro computer non sia infetto e volete rendere innocuo un disco di dubbia origine e potenzialmente pericoloso.*

- Partite normalmente facendo il boot come siete abituati e ottenendo il familiare prompt di sistema, di solito A> o C>.
- Inserite nel drive A il disco sospetto e copiate tutti i files su una direttrice che avrete opportunamente creato su C oppure su un disco inserito nel drive B e già formattato. NON USATE il comando DISKCOPY, bensì la COPY e non dimenticate di copiare anche i files contenuti nelle eventuali sottodirettrici del drive di partenza.
- Lanciate ora il comando FORMAT sul drive A, dove ancora deve trovarsi il disco sospetto, per ripristinare il contenuto della traccia zero. Se vi serve che questo disco sia utilizzabile per il boot del sistema usate FORMAT /S A:.
- Se volete, potete ora rieseguire la COPY di tutti i files sul disco decontaminato, che dovrebbe sempre trovarsi nel drive A.

```
PC Tools R2.06
                         Disk View/Edit Service
Path=A:
                 Relative sector being displayed is: 0000000

Displacement ————— Hex codes ——————————————————      ASCII value
 0000(0000)  EB 29 90 49 42 4D 20 20 33 2E 31 00 02 02 01 00   IBM 3.1
 0016(0010)  02 70 00 D0 02 FD 02 00 09 00 02 00 00 00 00 00
 0032(0020)  00 00 00 00 0F 00 00 00 00 01 00 FA 33 C0 8E D0
 0048(0030)  BC 00 7C 16 07 BB 78 00 36 C5 37 1E 56 16 53 BF
 0064(0040)  20 7C B9 0B 00 FC AC 26 80 3D 00 74 03 26 8A 05
 0080(0050)  AA 8A C4 E2 F1 06 1F 89 47 02 C7 07 20 7C FB CD
 0096(0060)  13 72 67 A0 10 7C 98 F7 26 16 7C 03 06 1C 7C 03
 0112(0070)  06 0E 7C A3 34 7C A3 2C 7C B8 20 00 F7 26 11 7C
 0128(0080)  8B 1E 0B 7C 03 C3 48 F7 F3 01 06 2C 7C BB 00 05
 0144(0090)  A1 34 7C E8 96 00 B8 01 02 E8 AA 00 72 19 8B FB
 0160(00A0)  B9 0B 00 BE BE 7D F3 A6 75 0D 8D 7F 20 BE C9 7D
 0176(00B0)  B9 0B 00 F3 A6 74 18 BE 5F 7D E8 61 00 32 E4 CD
 0192(00C0)  16 5E 1F 8F 04 8F 44 02 CD 19 BE A8 7D EB EB A1
 0208(00D0)  1C 05 33 D2 F7 36 0B 7C FE C0 A2 31 7C A1 2C 7C
 0224(00E0)  A3 32 7C BB 00 07 A1 2C 7C E8 40 00 A1 18 7C 2A
 0240(00F0)  06 30 7C 40 50 E8 4E 00 58 72 CF 28 06 31 7C 76

Home=beg of file/disk  End=end of file/disk
ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit
```

*Fig. 1 - Traccia zero senza virus.*

```
PC Tools R2.06
                         Disk View/Edit Service
Path=A:
                 Relative sector being displayed is: 0000000

Displacement ————— Hex codes ——————————————————      ASCII value
 0000(0000)  EB 1C 90 49 42 4D 20 20 33 2E 31 00 02 02 01 00   IBM 3.1
 0016(0010)  02 70 00 D0 02 FD 02 00 09 00 02 00 00 00 33 C0
 0032(0020)  8E D0 BC 00 7C 8E D8 A1 13 04 2D 02 00 A3 13 04
 0048(0030)  B1 06 D3 E0 2D C0 07 8E C0 BE 00 7C 8B FE B9 00
 0064(0040)  01 F3 A5 8E C8 0E 1F E8 00 00 32 E4 CD 13 80 26
 0080(0050)  F8 7D 80 8B 1E F9 7D 0E 58 2D 20 00 8E C0 E8 3C
 0096(0060)  00 8B 1E F9 7D 43 B8 C0 FF 8E C0 E8 2F 00 33 C0
 0112(0070)  A2 F7 7D 8E D8 A1 4C 00 8B 1E 4E 00 C7 06 4C 00
 0128(0080)  D0 7C 8C 0E 4E 00 0E 1F A3 2A 7D 89 1E 2C 7D 8A
 0144(0090)  16 F8 7D EA 00 7C 00 00 B8 01 03 E8 03 B8 01 02
 0160(00A0)  93 03 06 1C 7C 33 D2 F7 36 18 7C FE C2 8A EA 33
 0176(00B0)  D2 F7 36 1A 7C B1 06 D2 E4 0A E5 8B C8 86 E9 8A
 0192(00C0)  F2 8B C3 8A 16 F8 7D BB 00 90 CD 13 73 01 58 C3
 0208(00D0)  1E 06 50 53 51 52 0E 1F 0E 07 F6 06 F7 7D 01 75    PSQR
 0224(00E0)  42 80 FC 02 75 3D 38 16 F8 7D 88 16 F8 7D 75 22
 0240(00F0)  32 E4 CD 1A F6 C6 7F 75 0A F6 C2 F0 75 05 52 E8

Home=beg of file/disk  End=end of file/disk
ESC=Exit  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit      VIRUS
```

*Fig. 2 - Traccia zero con virus.*

Forse non è del tutto inutile sottolineare che se il disco sospetto conteneva una versione di sistema operativo più recente della vostra, in questa maniera la perderete, ma probabilmente è meglio così.

Caso B. *Il vostro computer potrebbe essere infetto e quindi propagare il virus.*
Se non avete il disco rigido praticamente rientriamo nel caso appena esaminato: SPEGNETE il computer e ripartite mettendo nel drive A il disco originale del Dos, quindi provvedete a decontaminare il disco che usate normalmente per il boot, che è l'unico in grado di propagare l'infezione. Se invece avete il disco rigido, allora la cosa si fa leggermente più complessa:

• SPEGNETE il computer e ripartite dal drive A, dove avrete inserito il disco originale del Dos. Fate bene attenzione a CHIUDERE lo sportellino del drive A, altrimenti vi ritrovereste in C> e dovreste spegnere (non ripartire con Ctrl + Alt + Del) e ricominciare daccapo.
• Ottenuto il prompt di sistema A> eseguite il comando

SYS C: [ENTER]

e quindi

COPY COMMAND.COM C: [ENTER]

Con queste operazioni distruggerete il sitema operativo che era sul disco rigido e lo sostituirete con quello preso dal disco che si trova nel drive A.
• Ripartite pure da dal drive C e continuate a lavorare come al solito.

Per il virus della pallina, in particolare, esiste anche un antidoto messo a punto dal poco scafato creatore del virus stesso. Si tratta di un programma che trovate sul disco Ultimobyte e che si chiama DEVIRUS.COM, il cui funzionamento risente a volte della mano inesperta del suo autore. Durante le nostre prove si è dimostrato quasi sempre in grado di ricostruire la traccia zero, ma non l'abbiamo mai lanciato (e sconsigliamo a chiunque di farlo) su un disco rigido.

## Palline, palline, palline

**Elementare, Watson!** In principio erano le palline, che ogni tanto comparivano sullo schermo del nostro monitor e che ci procuravano parecchia irritazione e una qualche preoccupazione. Poi cominciarono i sospetti, quando battendo dal drive C, ossia il nostro abituale drive di boot, l'innocente comando "DIR A:" vedemmo comparire un messaggio con cui il Dos ci informava dell'impossibilità di scrivere sul drive A. In effetti, il sistema operativo aveva tutte le ragioni del mondo, dato che il disco inserito nel drive A era protetto in scrittura, ma da quando — ci siamo subito chiesti — una Dir SCRIVE qualcosa da qualche parte? Evidentemente una entità aliena, non così astuta da occultarsi, aveva intercettato il comando e stava tentando di compiere azioni riprovevoli. La prima cosa che abbiamo fatto è stata quella di utilizzare immediatamente un altro disco di sistema per il boot, in attesa di riuscire a scoprire che cosa stava succedendo.

Un'altra circostanza, abbastanza casuale, ci aiutò parecchio a capire che doveva trattarsi di un virus "debole". Se cercate di fare il boot da un disco non appositamente preparato il Dos vi avvisa con uno specifico messaggio e vi chiede di inserire il disco corretto. Invece a noi capitò di inserire distrattamente in A un disco qualsiasi (non di boot), ma di NON vedere comparire detto messaggio, senza però naturalmente riuscire a partire. Fu a questo punto che quel poco di esperienza che abbiamo, unita a qualche buona lettura, ci mise sulla strada giusta: eravamo sicuramente stati contagiati, il virus non aveva una paternità illustre e doveva quasi certamente aver modificato qualcosa nelle tracce riservate al sistema operativo. Di qui, e prima ancora di entrare in possesso del programma DEVIRUS.COM, non fu difficile escogitare un sistema per ricostruire correttamente le tracce occupate dal Dos.

Per inciso, i due sintomi appena descritti dovrebbero essere abbastanza generici e avere buone probabilità di ripetersi in presenza di virus creati con la stessa tecnica e con la stessa scarsa attenzione ai particolari. Può anche essere interessan-

te verificare di tanto in tanto lo stato della memoria centrale (RAM) tramite il comando CHKDSK per vedere se lo spazio disponibile presenta una improvvisa e ingiustificata contrazione. Di solito i virus di questa specie non occupano molto, ma può darsi che riusciate a rendervi conto della strana scomparsa anche di due soli kappa. Queste metodologie sono tutte decisamente empiriche, ma hanno il grande pregio di non richiedere sofisticati strumenti di analisi e di poter quindi essere messe in atto con estrema semplicità.

**Un grazie di cuore.** Da un certo punto di vista dobbiamo essere grati all'anonimo creatore del virus della pallina, che con la sua imbecillità ci ha consentito di capire molte cose. Di grande importanza è stato, per esempio, aver scoperto che la propagazione avviene solo se il dischetto infetto è preparato per il boot. È in questo frangente infatti che il programma si comporta come il suo omonimo biologico trasferendosi su ogni supporto magnetico sul quale si compiano operazioni di lettura/scrittura fino allo spegnimento della macchina. Ciò accade perché al boot del computer viene portato in memoria centrale non solo il sistema operativo, ma anche il virus che agisce così come un programma residente, intercettando le chiamate al Dos e depositandosi su ogni disco che non sia già contagiato.

Pertanto, con un disco infetto, ma non di sistema, il pericolo di propagazione del contagio non esiste: è sufficiente decontaminare il disco incriminato per ovviare all'inconveniente. Visto che siamo in argomento sentiamo il dovere di avvertire i lettori che qualche copia del numero di Ultimobyte di Febbraio/88 potrebbe essere statisticamente sfuggita alla nostra pur scrupolosa verifica. Ora, il disco della rivista non è un disco di boot, ma a scopo cautelativo potete eseguire la procedura (Copy e Format) suggerita nella prima parte di questo articolo.

Il programma DEVIRUS, che pubblichiamo più che altro a titolo di curiosità in attesa che il suo autore si faccia avanti a reclamarne la proprietà come opera dell'ingegno, funziona da antidoto SOLO per il virus della pallina. La sintassi d'uso è molto semplicemente "DEVIRUS d:" dove "d:" è la lettera che identifica il drive sul quale si trova il disco infetto. Nel caso che il virus sia presente anche nella memoria centrale, il programma avverte di rifare il boot con un Dos non infettato prima di procedere con le operazioni di decontaminazione. Ribadiamo il consiglio di non lanciare DEVIRUS sul disco rigido, dato che l'arnese ha mostrato i suoi limiti in più di una circostanza. Talis pater, talis filius.

**Alle frontiere dell'assurdo.** Dobbiamo ammettere di avere qualche buon motivo per ammirare l'autore del programma della pallina. Come ha fatto costui ad acquistare tanta notorietà e quali sono i canali distributivi di cui si avvale e che gli hanno garantito una così buona copertura del territorio nazionale? Se intende rivelarcelo siamo disposti a pagargli una sostanziosa parcella per la consulenza di marketing. Per la verità, almeno a giudicare dalla dicitura "Versione 2.00" che fa bella mostra di sé nel programma di decontaminazione, l'individuo sembra sufficientemente ambizioso e stupido da voler persistere nella produzione di palline. In questo caso, non possiamo far altro che rimanere in attesa dei comunicati stampa relativi alle nuove versioni. Non mancheremo di pubblicarli, sicuri di rendere un buon servizio ai nostri lettori e a tutta la comunità degli utenti di computer.

Per concludere, dobbiamo purtroppo richiamare l'attenzione del lettore sul fatto che esistono altri tipi di virus, ben più pericolosi e difficili da estirpare. Questi sono programmi dall'apparenza molto normale, che vengono detti in gergo "cavalli di Troia" in quanto nascondono abilmente l'inganno. Fortunatamente possiamo opporre i nostri cavalli di Frisia, ossia programmi antisabotaggio in grado di rilevare i comportamenti anomali e potenzialmente pericolosi di qualsiasi altro programma e di avvisarci in tempo utile. Di questo parleremo in altra parte della rivista. **U**



# Cavalli di Frisia contro cavalli di Troia

## Da Swarthmore in Pennsylvania parte la prima crociata contro il sabotaggio organizzato. Tira aria di vittoria

Non conosciamo personalmente Andy Hopkins, eppure siamo in possesso del suo scarno biglietto da visita

*Andy Hopkins*
*526 Walnut Lane*
*Swarthmore, PA 19081*

e di due suoi formidabili programmi antisabotaggio, messi a disposizione di tutti gli utenti di PC secondo una formula esemplare, sulla quale ci piacerebbe molto che si fermassero per un istante a riflettere gli indigeni autori di software prezioso. La riportiamo prima in originale e poi nella nostra traduzione.

«In the spirit of cooperation with fellow PC users and hoping to discourage those whose idea of a joke is destroying other people's valuable data, I encourage you to make copies of this program and documentation and give it to anyone who may be succeptable to these pranksters. Users who frequently download BBS programs of unknown origin may find BOMBSQAD particularly useful. Complete rights to the the program itself, and the routines used in the program, however remain with the author, Andy Hopkins, through SWARTHMORE SOFTWARE SYSTEMS.»

«Nell'intento di collaborare con gli utenti di PC e sperando di scoraggiare chi si diverte a distruggere per gioco il lavoro di altri, vi invito a distribuire copie del mio programma e della relativa documentazione d'uso a chiunque ritenga di poter cadere vittima di questi burloni. Se vi rifornite spesso di programmi di origine sconosciuta, come quelli diffusi sulle reti BBS, potreste trovare particolarmente utile BOMBSQAD. Tutti i diritti sul programma e sulle routines usate appartengono comunque all'autore, Andy Hopkins, attraverso la SWARTHMORE SOFTWARE SYSTEM.»

Ogni commento ci appare superfluo.

I due programmi di cui parliamo in questo articolo servono per individuare i cosiddetti cavalli di Troia, ovvero programmi ad alto tasso di pericolosità — veri e propri ordigni esplosivi — sapientemente celati sotto la maschera dell'innocenza. CHK4BOMB è in grado di esaminare *preventivamente* un programma e di fornirvi un resoconto dettagliato in merito alle attività potenzialmente pericolose dello stesso. BOMBSQAD, invece, entra in azione *durante* il funzionamento di un programma e ne intercetta i comportamenti sospetti segnalandoli con appositi messaggi prima che divengano operativi, in modo da consentire all'utente di intervenire a neutralizzarli. Scendiamo nel dettaglio.

### I sintomi e la diagnosi

Il programma CHK4BOMB.EXE, che trovate sul disco con il pur involuto nome originale, si esegue battendo semplicemente

CHK4BOMB <nomefile>

al prompt del Dos, dove <nomefile> è il nome completo del file che desiderate analizzare. Il nostro amico produrrà su schermo la lista di tutte le stringhe ASCII contenute in <nomefile>, più un rapporto completo sulle attività po-

****WARNING**** This program writes to absolute sectors. The possibility exists to overwrite important data.

****WARNING**** This program FORMATS a disk! All data on the disk could be lost!

****WARNING**** This program uses the ROM BIOS routines for direct disk access! This program COULD format a disk or write to certain sectors without updating the directory or File Allocation Table.

**DO NOT RUN** this program until checked by an expert, unless you are familiar with the author or company.

****ATTENZIONE**** Questo programma scrive sul disco indirizzando i settori in modo assoluto. Esiste la possibilità che vengano ricoperti dati importanti.

****ATTENZIONE**** Questo programma FORMATTA un disco! Ciò potrebbe provocare la perdita di tutti i dati sul disco in questione!

****ATTENZIONE**** Questo programma usa le routines BIOS contenute nella memoria ROM per accedere direttamente al disco! Il programma POTREBBE formattare un disco o scrivere su alcuni settori senza aggiornare la direttrice o la File Allocation Table (Tavola di allocazione dei files, una specie di indice del disco).

**NON MANDATE IN ESECUZIONE** questo programma prima di farlo controllare da un esperto, a meno che non ne conosciate con certezza la provenienza.

*Fig. 1 - La diagnosi di CHK4BOMB.*

tenzialmente pericolose previste dal programma in esame. Gli eventuali messaggi di avvertimento in Inglese sono molto chiari, ma riportiamo anche la traduzione in Italiano ( vedi Figura 1), a costo di essere tacciati di pedanteria.

Vogliamo sottolineare che possono esistere "bombe" non rivelate da CHK4BOMB, dato che spesso il codice di un programma è in grado di automodificarsi in funzione di condizioni variabili di volta in volta e riscontrabili solo durante l'effettivo funzionamento. Pertanto, a seguito di una diagnosi tanto precisa da lasciare veramente poco spazio all'immaginazione, possiamo comunque decidere di lanciare il programma incriminato, con la tranquillità che ci deriva dall'avere messo a guardia del nostro PC l'invincibile BOMBSQAD, di cui passiamo subito ad occuparci.

## Abbaia e morde

BOMBSQAD.COM è una specie di virus all'incontrario: la tecnica è la stessa, opposti sono gli obiettivi. Lo scopo che infatti BOMBSQAD — di nuovo il nome è impossibile, ma il grande rispetto per l'autore ci ha indotti a mantenerlo — si prefigge è quello di piazzarsi in memoria centrale (RAM) e di intercettare tutte le chiamate al BIOS (Basic Input Output System), avvertendoci di quello che sta per accadere e chiedendoci se desideriamo o meno interrompere il programma sospetto, prima che questo possa provocare danni.

La sintassi è "BOMBSQAD [RWVFU]" e prevede di bat-

tere BOMBSQAD seguito da uno o più parametri opzionali, che determinano le condizioni in base alle quali bloccare il programma attualmente in esecuzione:

- R per arrestare l'esecuzione su ogni richiesta di LEGGERE un settore
- W per arrestare l'esecuzione su ogni richiesta di SCRIVERE su un settore
- V per arrestare l'esecuzione su ogni richiesta di VERIFICARE un settore
- F per arrestare l'esecuzione su ogni richiesta di FORMATTARE una traccia
- U per disattivare BOMBQSQAD. Da notare che la memoria occupata non verrà comunque rilasciata fino al boot successivo.

Se non si forniscono parametri, ossia se si batte BOMBSQAD da solo, esso rimane attivo, pur non arrestandosi su alcuna richiesta di accesso al disco.

Una prova utile a chiarire il funzionamento del programma potrebbe essere

BOMBSQAD R

con cui si richiede l'arresto su ogni tentativo di accesso a disco in LETTURA (R sta per READ). Ora, con BOMBSQAD reso così residente in memoria, eseguite l'insospettabile comando DIR e osservate il comportamento. Appena BOMBSQAD si accorge che qualcuno (la Dir nel nostro esempio) tenta di leggere dal

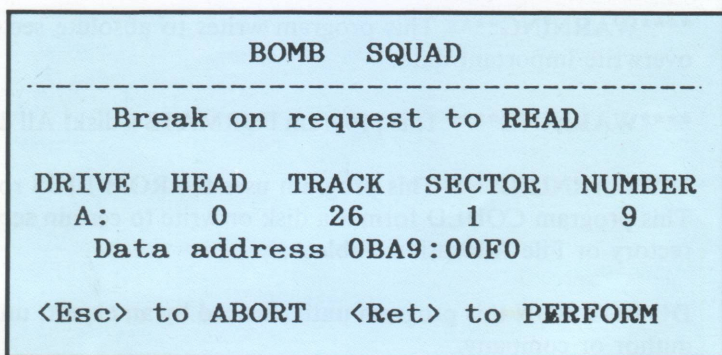


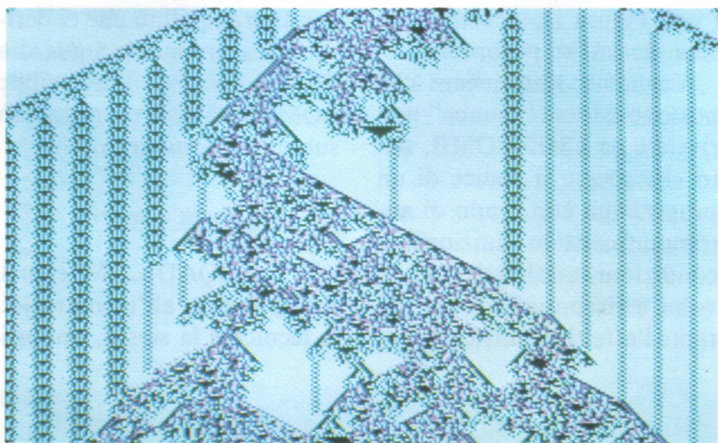

*Fig. 2 - Così BOMBSQAD suona l'allarme.*

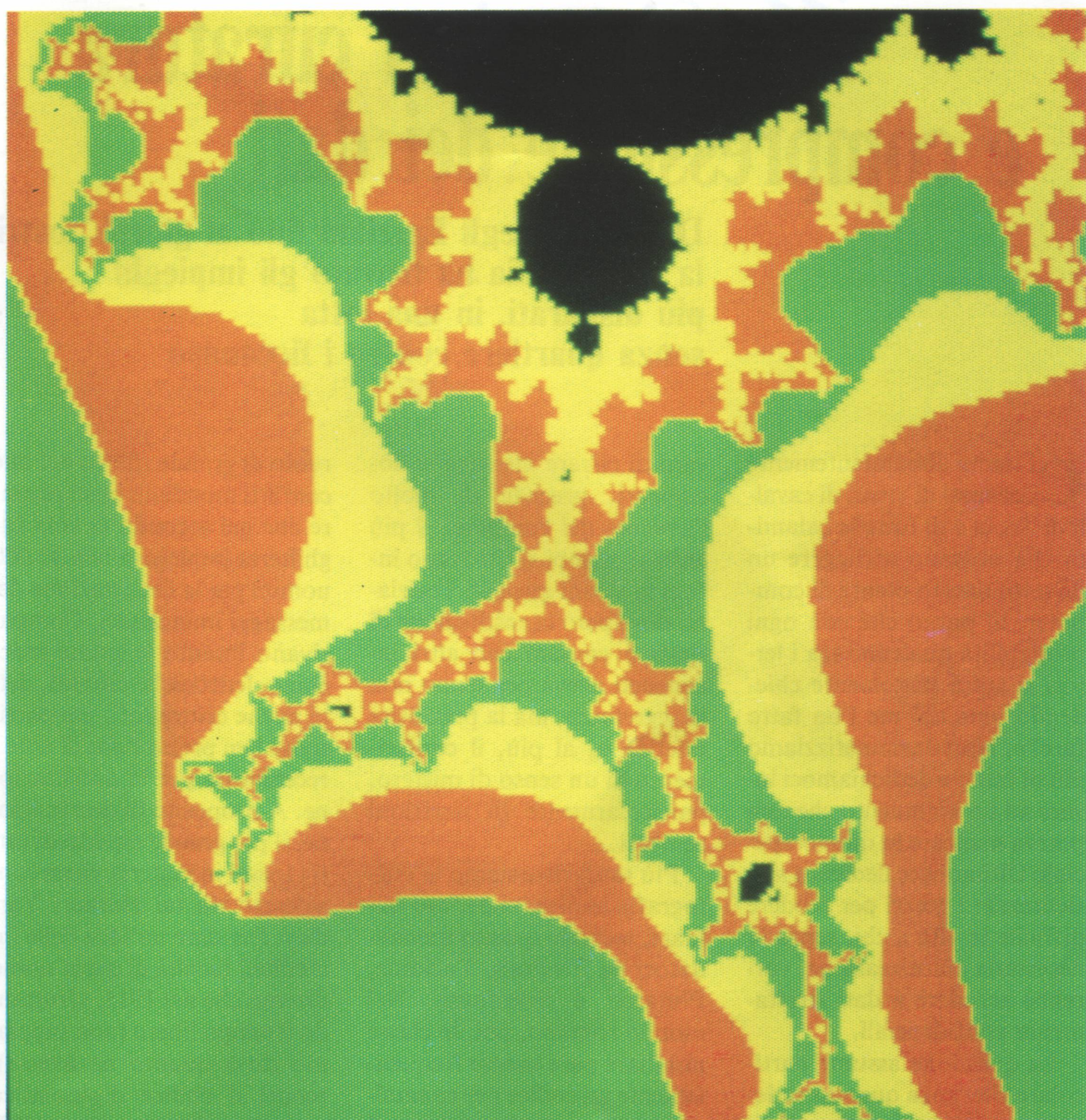
disco, intercetta la richiesta e, prima che questa venga esaudita, fa apparire sullo schermo un messaggio del tipo mostrato in Figura 2. A questo punto avete la possibilità di scegliere tra

- battere il tasto ESC per impedire che avvenga l'operazione su disco, ossia la READ nel caso in esame
- battere il tasto RETURN per dare via libera all'esecuzione dell'operazione di lettura richiesta dalla Dir.

L'esempio non ha alcuna utilità pratica, ma dimostra tutta la potenza del programma. In termini generali, quando BOMBSQAD intercetta un richiamo delle routines BIOS controlla se è presente la condizione di arresto e, in caso negativo, trasferisce direttamente il controllo alla routine chiamata, altrimenti fa comparire il messaggio della Figura 2. Il significato delle diciture è il seguente:

- DRIVE è la lettera (A/D) che identifica il drive sul quale è stata richiesta l'operazione
- HEAD è il numero della testina di lettura/scrittura interessata. Per le unità a floppy questo numero coincide con la faccia (0/1)
- TRACK è il numero del cilindro o traccia, espresso in notazione decimale (0/39 per i floppy)
- SECTOR è il numero del primo settore interessato nell'am-





bito della traccia (normalmente 1/9)

• NUMBER è il numero totale di settori coinvolti nell'operazione richiesta

• DATA ADDRESS identifica la zona di memoria centrale (gli indirizzi sono in notazione esadecimale) dove sono memorizzati o da dove sono letti i dati

Un ultimo avvertimento. BOMBSQAD è un programma residente in memoria, ma non tenta di reinstallarsi se è già installato. Inoltre, esso si arresta solo in base ai parametri forniti sulla riga dei comandi all'atto dell'ultima esecuzione. Tutto questo vuole semplicemente significare che se si parte ad esempio con "BOMBSQAD F" per ottenere l'arresto *solo* su un richiamo della FORMAT e si vuole in seguito l'arresto *anche* sulla WRITE, occorre rilanciare "BOMBSQAD FW".

Andy Hopkins, l'autore dei due programmi descritti in questo articolo e pubblicati sul disco allegato, abita a Swarthmore in Pennsylvania. Può darsi che qualcuno si senta in debito nei suoi confronti. U

# Sistemi di cifratura e compressione dei dati

**Dai tempi degli Egiziani fino ai giorni nostri la crittografia ha trovato gli impieghi più disparati, in una lotta senza quartiere contro i ficcanaso**

Ci siamo abbondantemente occupati di virus, di cavalli di Troia e di tutte le calamità che possono affliggere un povero, onesto utente di computer, al punto che con ogni probabilità qualcuno tra i lettori si starà tristemente chiedendo «ma chi me l'ha fatto fare?». Non drammatizziamo più di tanto e dedichiamoci invece ad un argomento che non poteva mancare in questo Speciale Ultimobyte dedicato alla sicurezza: i mezzi per rendere difficile la vita a chi, senza la necessaria autorizzazione, vorrebbe accedere a dati strettamente confidenziali.

La questione assume particolare rilevanza quando si devono trasmettere dati sulle linee telefoniche oppure quando, specialmenti in ambienti di multiutenza, non si ha modo di verificare se chi accede ai dati è autorizzato o meno a farlo. In questi casi è utile avere la possibilità di cifrare i propri documenti in modo da impedire ad estranei di trarre qualche vantaggio dalla loro lettura.

L'arte della crittografia, ovvero di cifrare messaggi e documenti, precede di molto l'avvento del computer. I più antichi esempi si ritrovano infatti in alcuni geroglifici egiziani, dove però la sostituzione di simboli comuni con altri inconsueti aveva per scopo non la segretezza, ma la preziosità estetica o, al più, il conferimento di un senso di mistero, particolarmente in iscrizioni tombali.

Più tardi ritroviamo la crittografia impiegata per uso militare, secondo quanto tramandatoci da Erodoto, Tucidide, Plutarco e Senofonte. Nel mondo romano, poi, la classe nobiliare pare usasse frequentemente un codice per comunicare e Cesare stesso narra nel De bello gallico di aver fatto ampio ricorso alla crittografia. L'interesse per la crittografia diminuì alquanto nel Medio Evo per poi fare nuovamente capolino durante il Rinascimento. All'epoca di Luigi XIV venne usato un codice basato su 587 chiavi scelte casualmente per crittografare i messaggi segreti del governo.

Questa scienza ebbe poi un ruolo di grande rilievo nei due conflitti mondiali: basti pensare che nel secondo la sola Inghilterra impiegava ben 30.000 uomini per la decrittazione dei messaggi intercettati. Comparivano intanto le prime macchine elettroniche cifranti, dette anche crittografi, cui corrispose ben presto l'uso di apparecchiature per la decrittazione. A proposito di decrittazione, il più grande esperto di tutti i tempi in materia viene considerato un tal Herbert Yardley. Per dare un'idea delle incredibili facoltà di quest'uomo diremo che nel 1915, sfruttando il tempo libero (non sappiamo dirvi quanto ne avesse), scoprì il codice diplomatico americano, mentre nel 1922, pur non conoscendo una sola parola di Giapponese, riuscì a decifrare anche il codice usato dai diplomatici dell'impero del sol levante basandosi sulle tavole di frequenza relative alla loro lingua.

## Mantenere il segreto

I crittografi automatici, per quanto complicati potessero

| Alfabeto normale | Alfabeto di sostituzione |
|---|---|
| A | F |
| B | I |
| C | D |
| D | S |
| E | M |
| F | R |
| G | A |
| H | O |
| I | T |
| J | C |
| K | U |
| L | E |
| M | H |
| N | B |
| O | L |
| P | J |
| Q | V |
| R | K |
| S | W |
| T | P |
| U | X |
| V | G |
| W | Q |
| X | Z |
| Y | N |
| Z | Y |

U L T I M O B Y T E
diviene
X E P T H L I N P M

*Fig. 1 - Cifratura per sostituzione.*

essere, si basavano su codici costruiti secondo regole determinate e quindi decrittabili, almeno in linea teorica. Con l'avvento del computer lo sviluppo dei metodi di cifratura ricevette un impulso decisivo. Il più noto di tali metodi è oggi il DES (Data Encryption Standard), che ha anche ricevuto l'approvazione dall'americano NBS (National Bureau of Standards). In generale, comunque, i numerosi sistemi crittografici utilizzabili si possono raggruppare in due grandi categorie: il sistema alfabetico e quello a codice. Il primo opera su singole lettere o su gruppi di poche lettere seguendo due metodi fondamentali

1) la sostituzione, con la quale si mette al posto di una lettera del testo in chiaro, ogni volta che la si incontra, un'altra lettera, cifra o simbolo (vedi Figura 1)

2) la trasposizione, con la quale si cambia posto a ciascun carattere del testo in chiaro in base ad una qualche regola convenzionale (vedi Figura 2)

Ovviamente nulla impedisce di combinare i due metodi, a tutto vantaggio della sicurezza.

Nel sistema a codice si utilizzano appositi volumi, chiamati repertori o cifrari, che

Una possibile regola di trasposizione

*Dividere la parola in coppie di lettere a partire da sinistra, quindi invertire l'ordine delle lettere in ogni coppia così formatasi.*

Parola da cifrare con la regola precedente

U L T I M O B Y T E

Risultato della cifratura

L U I T O M Y B E T

Risultato della doppia cifratura, ottenuta applicando, dopo la trasposizione, la sostituzione con l'alfabeto della Figura 1

E X T P L H N I M P

*Fig. 2 - Trasposizione e sostituzione combinate.*

contengono una lista di elementi chiari, a ciascuno dei quali corrisponde un gruppo di cifre, e una lista inversa per la successiva decifrazione del messaggio. Anche questo è una specie di procedimento per sostituzione, che si effettua però su sillabe, parole e intere frasi, a cui vengono fatti corrispondere gruppi cifranti. Quando si usa il computer, come nel caso del nostro programma ENCRYPT, si ricorre di norma alla tecnica della manipolazione a livello del bit, che, combinata ad esempio con la trasposizione, mette al riparo dalla possibilità che si sfruttino le tavole di frequenza della lingua per decrittare il messaggio.

Per comprensibili motivi di segretezza non possiamo entrare nel merito dell'algoritmo usato dal programma ENCRYPT, che prevede la sintassi seguente:

ENCRYPT chiave <file da cifrare >file cifrato

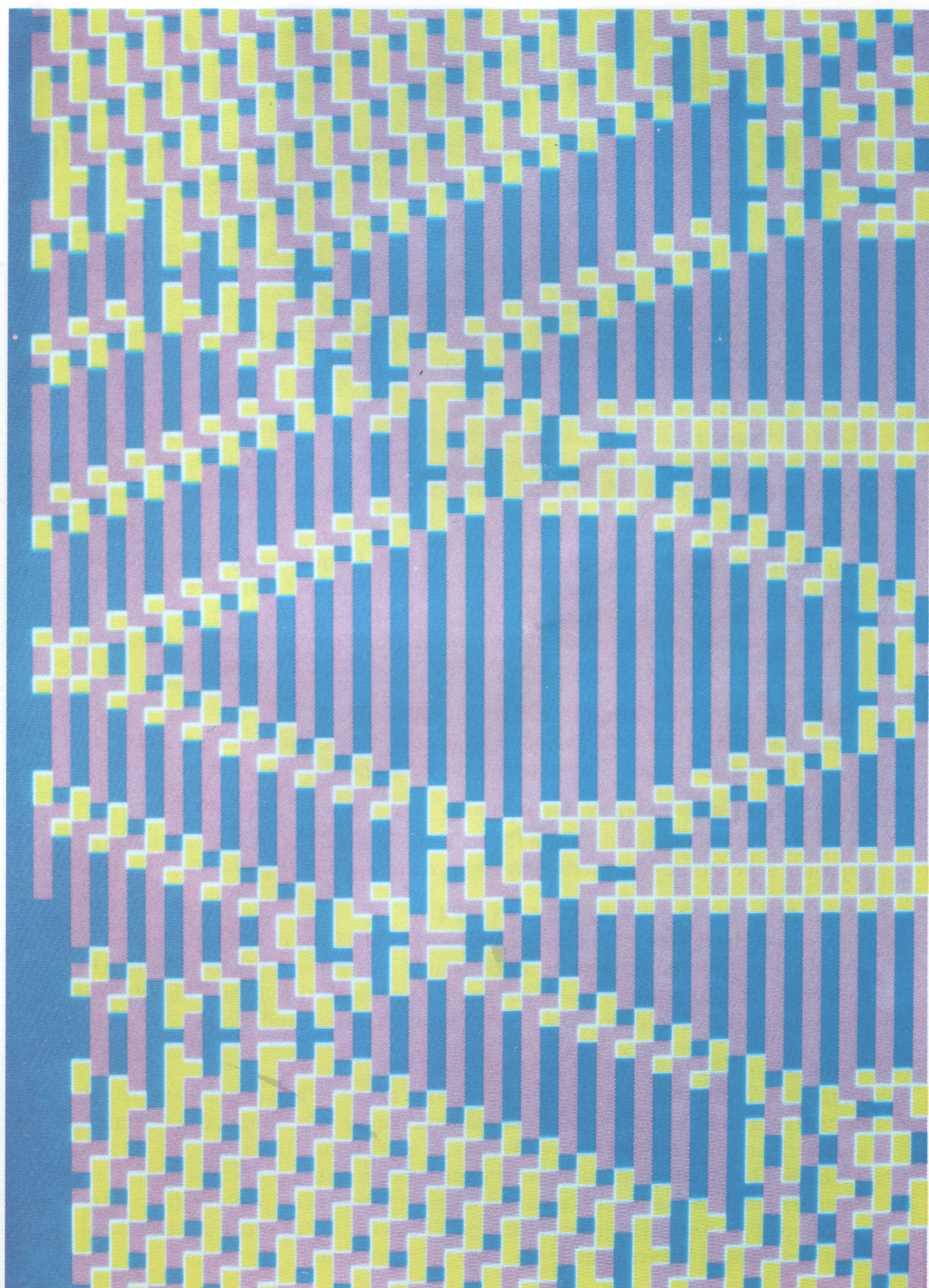
dove "chiave" sta per una qualsiasi parola chiave, senza conoscere la quale le probabilità di ricostruire il testo in chiaro sono terribilmente misere. I simboli "<" e ">" sono gli indicatori di ridirezione del Dos e significano, rispettivamente, "prendi da" e "metti in". Esempio chiarificatore

ENCRYPT mamma <miofile.txt >miofile.enc

dove viene letto in input il file in chiaro di nome miofile.txt e creato in output su disco il file di nome miofile.enc, cifrato con chiave "mamma". Lo stesso programma, con la stessa sintassi, effettua il processo inverso di decifratura

ENCRYPT mamma <miofile.enc >chiaro.mio

È evidente che per poter de-



# Dalla Libreria PC-SIG

## Tra i 1000 dischetti della Libreria PC-SIG abbiamo selezionato tutti quelli che hanno a che vedere in qualche modo con il problema della sicurezza di dati e programmi. Ve li descriviamo brevemente di seguito.

**Cod. 112 - COMPUTER SECURITY PACKAGE**
Una serie di programmi per la cifratura dei files. Molto completo e ben documentato, ma poco adatto a chi è alle prime armi.

**Cod. 230 - THE CONFIDANT**
Uno dei migliori dischi di tutta la Libreria. Due sistemi di cifratura: DES (Data Encrypt Standard) per la massima sicurezza e una seconda procedura, un po' meno sicura e molto più veloce. Ottima la documentazione.

**Cod. 482 - ENCODE/DECODE**
Contiene programmi di cifratura e decifratura in formato sorgente (Turbo Pascal), per cui può risultare molto utile a chi cerca spunti per realizzare un proprio sistema di sicurezza. L'interesse del programma consiste nel fatto che mantiene la formattazione dei files prodotti con i Word Processors anche quando vengono trasmessi via posta elettronica.

**Cod. 490 - MICRO-COMPUTER DATA SECURITY**
Compilation di utilities che ampliano la capacità del DOS in termini di sicurezza. Tutti i programmi sono accompagnati da un file di documentazione.

**Cod. 491 - CRYPTANALISYS HELPER**
Programma di aiuto per decifrare files cifrati. Gli algoritmi sono basati sulla frequenza delle lettere e si riferiscono sostanzialmente alla lingua inglese.

**Cod. 569 - PC-CODE3 AND PC-CODE4**
Per cifrare dati e programmi sia in ambiente MS-DOS che in ambiente Microsoft Xenix. I programmi sono scritti in Fortran-77 (Versione 3.3 della Microsoft) e i moduli oggetto possono essere direttamente collegati (LINK) alle librerie Fortran dell'MS-DOS o dello Xenix, senza bisogno di ricompilazione.

**Cod. 893 - PRIVATE LINE AND WEAKLINK**
Programma di cifratura/decifratura conforme al Data Encrypt Standard del National Bureau of Standards. Prevede anche la doppia cifratura, ossia la cifratura (preferibilmente con una chiave diversa) di un file già cifrato.
WEAKLINK permette di collegare tramite la porta seriale due PC per il trasferimento di dati tra macchine che hanno supporti fissi o incompatibili: tipico il trasferimento da una macchina con drive da 5 pollici ad un'altra con drive da 3 pollici. La velocità è selezionabile tra 1200 e 115.000 baud.

# TDK
# PROFESSIONAL FLOPPY DISK

Questo disco di pochi centimetri quadrati potrebbe contenere centinaia di ore del vostro lavoro, un valore spesso incalcolabile.
**TDK LO SA!**

TDK, leader mondiale del settore, ha investito il meglio dei suoi 35 anni di esperienza nella registrazione magnetica per produrre i Floppy Disk migliori del mondo, i più sicuri, garantiti uno per uno al 100%*.

I Floppy Disk TDK da 3 ½, 5 ¼ e 8 pollici sono disponibili in 10 versioni per qualsiasi esigenza.

*I controlli più severi su tutti i dischi TDK superano ampiamente le normative standard imposte da IBM, Shugart, HAMSI, ECMA, ISO e JIS.



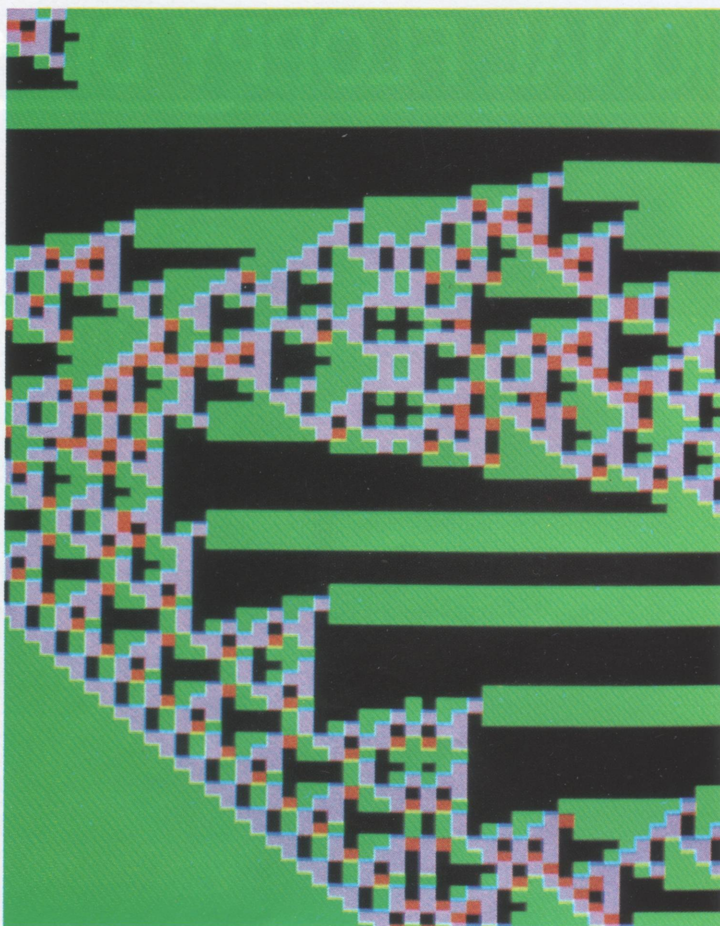


**TDK** perchè i Floppy Disk non sono tutti uguali

I Floppy Disk TDK sono distribuiti da: EPSON-SEGI S.p.A.
Milano, Via Timavo 12, Tel. 02-6709136 - Padova, Tel. 049-8070870
Bologna, Tel. 051-245619 - Roma, Tel. 06-8395766




STUDIO MARTINETTI



cifrare un file cifrato con ENCRYPT occorre non solo essere in possesso del programma, ma anche conoscere la chiave esatta. E ricordate, la chiave ''mamma'' è diversa da ''Mamma''.

## Cifrare vuol dire risparmiare

Sempre in tema di manipolazioni (di testi, non genetiche), esiste la possibilità di sfruttare l'eccesso di bit che il PC usa per rappresentare i caratteri e catturare così i due classici piccioni con una fava: cifrare il testo, anche se in maniera assai poco sofisticata, e ridurne contemporaneamente la lunghezza. Questo è precisamente quello che fa il programma COMPRESS. A che cosa serve? Sostanzialmente è stato pensato a beneficio di coloro che usano le linee telefoniche per trasmettere dati. Accorciare il testo mediamente del 12.5% può significare un discreto risparmio sulla bolletta telefonica.

In secondo luogo, il semplice fatto di poter mettere su un disco più dati di quanti apparentemente ce ne possono stare ha la sua importanza, non tanto per il costo ormai trascurabile del dischetto, quanto per una più razionale organizzazione dei files sui dischi. Ne sa qualcosa chi si è trovato a dover salvare su floppy un file di 370k bytes o, caso forse più disperato, a dover utilizzare un secondo floppy per metterci l'ultima routine della collezione, che sarebbe tanto utile conservare su un solo disco.

La sintassi di COMPRESS è la seguente

COMPRESS inputfile outputfile [c/d]

dove ''inputfile'' e ''outputfile'' indicano rispettivamente i nomi completi del file da leggere in input e di quello da produrre in output, mentre le lettere ''c'' o ''d'' specificano se l'operazione da compiere è la compressione o l'inverso. Esempio

COMPRESS C:file1.txt A:file1.txt c

per copiare dal drive C al drive A il file di nome file1.txt in forma compressa. Può essere interessante notare che qualora file1.txt fosse in formato ASCII puro, potremmo usare prima COMPRESS e poi ENCRYPT per aumentare la sicurezza, a patto però di ricordare con precisione tutte le manipolazioni compiute. Altrimenti metteremmo in difficoltà sicuramente i ficcanaso, ma probabilmente anche noi stessi. Ci sarebbe da ridere! U




## Il filtro Polaroid elimina il riverbero e riduce i costi

Il riverbero e la mancanza di contrasto sullo schermo possono causare problemi di salute agli operatori: male alla testa, agli occhi, vertigine.

Il risultato è scarsa produttività, errori ed al limite assenteismo.

Il nuovo filtro Polaroid CP50 elimina il riverbero e migliora il contrasto. Altri filtri fanno l'una o l'altra cosa ma non entramnbe.

Certamente si potrebbe tentare di trovare una soluzione al riverbero cambiando il sistema di illuminazione dell'ufficio: cioè tende e mobili.

Tutto ciò però non aumenterebbe il contrasto e quale sarebbe il costo?

Il CP50 è un filtro di polarizzazione resistente e leggero che assorbe la luce che cade sullo schermo non facendola riflettere negli occhi dell'operatore. E' altresi molto efficace nell'aumentare il contrasto.

Il CP50 ha diverse dimensioni e si adatta facilmente, senza utensili, su quasi tutti i tipi di video.

Una volta adattato non c'è più bisogno di cambiarlo.

**Polaroid**

**datamatic**
TRATTA BENE IL TUO CALCOLATORE

20124 MILANO - Via Volturno, 46
Tel. (02) 6073876 (5 linee r.a.)
Telex 315377 SADATA I
Filiale ROMA: Via Città di Cascia, 29
Tel. (06) 3279987 (4 linee r.a.)

Polaroid e CP-50/CP-70 sono nomi e marchi registrati esclusivamente dalla Polaroid Corporation.

# La difficile arte di ben cancellare

**Contrariamente a quanto si potrebbe credere i comandi di cancellazione previsti dal Dos si guardano bene dal cancellare. Vi proponiamo un rimedio portentoso, che stupirebbe persino Peter Norton**

Il sistema operativo, sia esso MS o PC-DOS, mette a disposizione ben due comandi per cancellare files dal disco. Già questa abbondanza risulta di per sé piuttosto inspiegabile e bisogna risalire fino al CP/M, da cui storicamente il DOS discende, per trovare una giustificazione all'esistenza dei sinonimi DEL ed ERASE, il secondo dei quali, forse reo di portare un nome troppo lungo, ci risulta da tempo caduto in disgrazia presso gli utenti. C'è poi da considerare che i due compari si limitano a togliere il file dalla direttrice attiva, senza effettivamente cancellarlo dal disco, tanto che non è difficile riportarlo in vita con strumenti quali Norton Utilities o Pctools, largamente diffusi tra i programmatori di professione.

Chi programmatore di professione non è saprà sicuramente apprezzare il nostro UNDEL, che consente per l'appunto di recuperare un file precedentemente cancellato con DEL o ERASE. La sintassi è semplicemente UNDEL <nomefile> e non è previsto l'uso dei caratteri jolly * e ?, per cui occorre forzatamente ricordare il nome completo del file che si vuole resuscitare. Per amore di precisione, ma senza approfondire ulteriormente l'argomento, diciamo che in effetti potete permettervi il lusso di dimenticare la prima lettera del nome del file e indicarne una a caso. In altre parole, se avete distrattamente eseguito "del tuofile.exe" potete rimediare anche con "undel suofile.exe", che riporterebbe in vita *tuofile* ribattezzandolo *suofile*. Ricordate, tutto questo vale solo per la prima lettera del nome.

A conclusione di questa disquisizione sulla Del e prima di passare a vedere come si possono sconfiggere le Norton Utilities, le Pctools e la nostra Undel, vi esortiamo a tenere nella massima considerazione il fattore tempo. La Del e la Erase, come ampiamente ribadito, non cancellano il file dal disco, però danno carta bianca al sistema operativo per la gestione dello spazio occupato dal file in questione. Questo vuol dire che bisogna eseguire la Undel *prima* che il Dos assegni detto spazio ad un nuovo file, che ricoprirebbe totalmente o parzialmente il predecessore. Naturalmente il Dos non si diverte a spostare i files da una parte all'altra del disco motuproprio, ma nulla gli vieta, per esempio, di destinare lo spazio liberatosi a seguito di una Del ad un file da voi trasferito con una Copy nella stessa direttrice. È tutta questione di tempo!

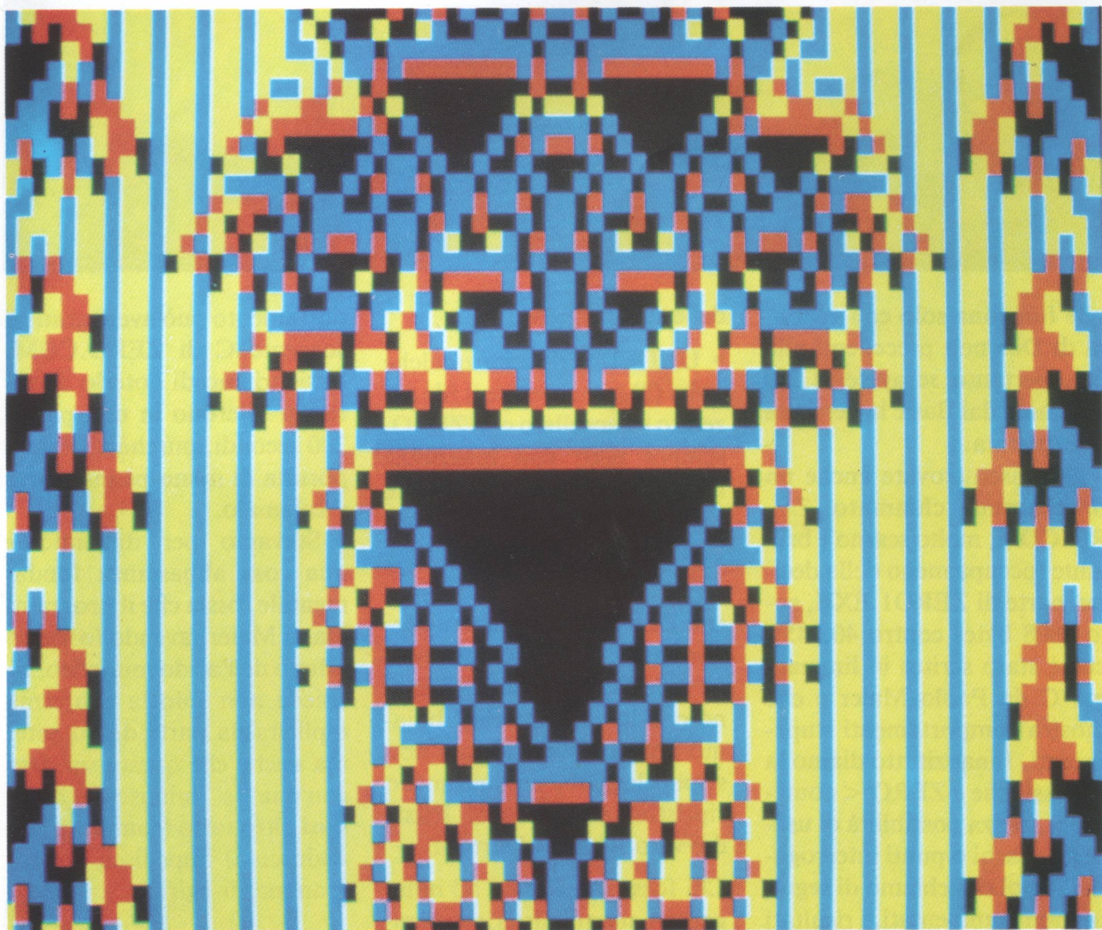
## Voglio la mia privacy

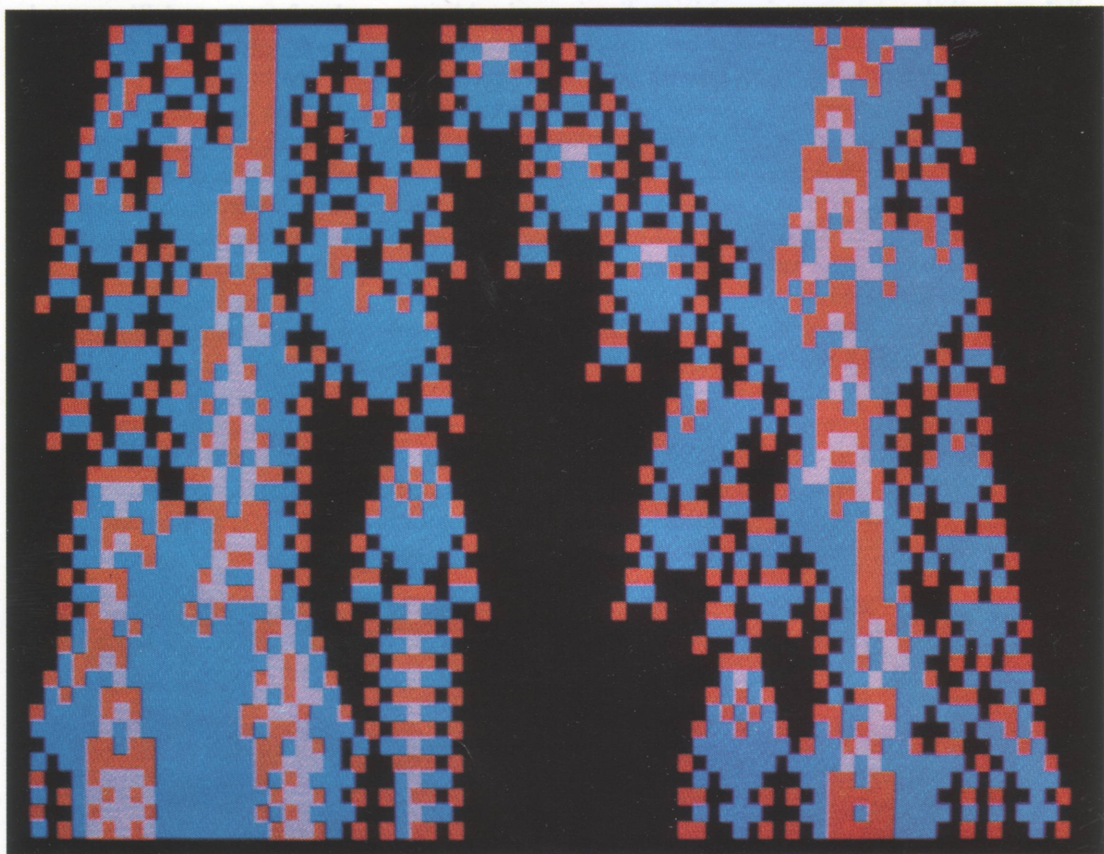
Visto che la Del non basta per sottrarre a sguardi indiscreti i vostri dati e visto che questo Speciale Ultimobyte è dedicato alla sicurezza, abbiamo pensato di fornirvi gli strumenti atti ad azzerare un file prima di toglierlo dalla direttrice attiva con i comandi Del o Erase. Per eliminare in partenza il dubbio — ma come si fa a recuperare un file se non se ne conosce almeno il nome? — che immaginiamo formarsi

nella mente di alcuni dei nostri lettori, vi diciamo che tramite diavolerie come le già menzionate Norton Utilities o Pctools non solo si ottiene la lista completa dei files su cui è stata eseguita la Del, con nome ed estensione, ma si riesce anche a sapere quale tra questi è automaticamente recuperabile in quanto non ancora sovrascritto. La nostra UNDEL, che da questo punto di vista è meno potente, recupera invece solo un file alla volta e solo se le viene comunicato il nome.

La nostra risposta alla richiesta di privacy è addirittura banale nella sua concezione: porre a zero tutti i bytes del file che vogliamo cancellare e lasciare pure che gli indiscreti si divertano ad andare a ficcare il naso nella desolante e poco significativa sequenza di spazi vuoti che così si ottiene. Il programma adatto allo scopo si chiama ZERO1 e si trova sul disco sia nel formato sorgente Basic (ZERO1.BAS), sia sotto forma di eseguibile (ZERO1.EXE), nell'intento di rispettare le esigenze del programmatore che cerca spunti da sfruttare e dell'utente che vuole solo risultati immediati.

Per lanciare il programma bisogna battere ZERO1 al prompt del Dos e rispondere alle domande che compaiono sullo schermo. Si può cancellare un file per volta e non sono ammessi i caratteri jolly * e ?. I files trattati con ZERO1 possono essere riportati in vita con il comando UNDEL, con le Norton Utilities, con Pctools o con qualsiasi altro sistema, ma risultano sempre e comunque rigorosamente vuoti. ZERO1 in formato esegui-





bile funziona solo con versioni di Dos non precedenti alla 2.1, pertanto se avete la 2.0 chiamate dal Basic la versione interpretata.

Sul disco trovate anche un programma chiamato ZERO.COM, molto scarno e brillante (occupa meno della decima parte di ZERO1.EXE, solo 3808 bytes contro 40.745), che è stato scritto in linguaggio C da Paolo Maier e che mostra comportamenti stupefacenti. Innanzitutto diamo la sintassi, che è ZERO <nomefile>, senza possibilità di usare asterischi o punti interrogativi, e poi elenchiamo di seguito, non commentati, i risultati delle nostre prove:

- UNDEL è riuscita qualche volta (?) a recuperare il file azzerato e cancellato con ZERO, sempre però con lunghezza nulla. Praticamente l'effetto è simile a quello ottenuto con ZERO1.
- Per Pctools il file cancellato con ZERO non esiste più. Meglio di ZERO1, anzi ottimo.
- Per le Norton Utilities (almeno con la versione che abbiamo noi) il file esiste, ma non si può leggere, né tantomeno ripristinare sul disco. Esiste davvero il mago Norton?

Chi fosse interessato ad indagare su questo misterioso comportamento può avere gratis il sorgente C di ZERO.COM. Assicuriamo di poterlo dettare per telefono in non più di 200 secondi, purché abbiate a portata di mano penna, carta e calamaio.

Stavamo per dimenticare una cosa abbastanza fondamentale, ossia che il programma di Maier, avendo lo stesso effetto dell'acido muriatico, richiede non solo la conferma esplicita da parte dell'utente, ma anche che questa sia data con una ''s'' minuscola: qualsiasi altro tasto (compresa la S maiuscola) impedisce al programma di agire. U

# ABBONATEVI

**Ultimobyte**

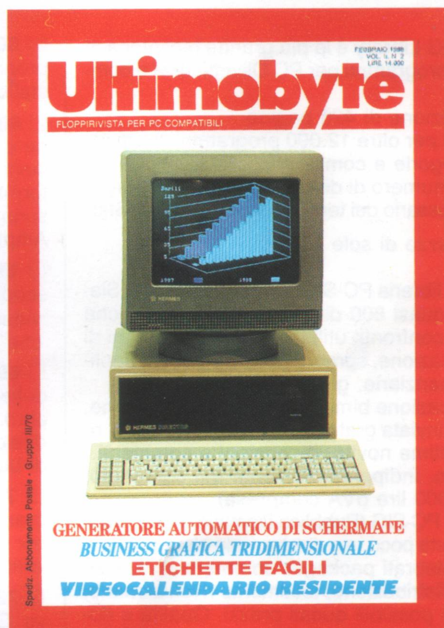
**360K di programmi al mese**

**Abbonarsi ora vuol dire risparmiare**

**1 Anno Solo L. 126.000**

**Ritagliare e spedire in busta chiusa a:**

**Ultimobyte Editrice S.r.l.**
**Via A. Manuzio, 15**
**20124 MILANO**
**Tf. 02/6597693**




**SI** mettete in corso un abbonamento a mio nome. Ho diritto a ricevere Ultimobyte per 1 anno (11 numeri) a L. 126.000 con un risparmio di 28.000 lire sul prezzo di copertina

Nome/Cognome ....................

Indirizzo ....................

Città .................... PR .......... CAP ..........

Pagamento
☐ Assegno allegato
☐ Vaglia postale (fotocopia allegata)



Offerta valida solo per l'Italia a tutto Aprile 1988

# The PC-SIG Library

## Poche chiacchiere, tanto software

The PC-SIG Library è la più grande biblioteca al mondo di programmi per PC Olivetti, IBM e compatibili.
Nuova edizione di 420 pagine.
705 dischi per oltre 12.000 programmi suddivisi in 27 categorie e commentati.
Indici per numero di disco, per titolo e per argomento. Glossario dei termini, da ADA a WordStar.

Nuovo prezzo di sole 25.000.

Da oggi la libreria PC-SIG è ancora più ricca. Siamo già a quasi 800 dischi, con una scelta che non teme confronti: utilities, giochi, linguaggi di programmazione, spreadsheet, WP, corsi, applicazioni finanziarie, grafica e altro.
La pubblicazione bimestrale PC-SIG Magazine, che viene inviata gratuitamente agli Associati, riporta le utlime novità, recensioni e commenti.
Ogni disco, indipendentemente dal contenuto, costa 18.000 lire (IVA compresa).
Il software PC-SIG (Pubblico Dominio e User Supported) costa poco, ma spesso vale almeno quanto i più celebrati packages commerciali. È il sistema di distribuzione, totalmente rivoluzionario, che rende possibili questi prezzi. Qualità e documentazione (sempre in Inglese, su disco) sono ai massimi livelli.

### Alcune Novità

☐ **499 PROCOMM** Semplicemente uno dei migliori programmi per le comunicazioni. Lo trovate anche nell'elenco ''Il Meglio del 1986'' pubblicato da PC Magazine americano.

☐ **577-578 C TUTOR** Corso completo per imparare a programmare in linguaggio C. Il disco 577 contiene i testi e il 578 gli esempi didattici, oltre ad una discussione sui vari compilatori C in commercio.

☐ **579-580 PASCAL TUTOR** Corso introduttivo sul linguaggio Pascal (anche Turbo Pascal) per principianti ed esperti. Il disco 579 contiene i testi e il 580 gli esempi didattici.

☐ **583 1-2-3. THE WHITEROCK ALTERNATIVE** Semplifica l'accesso e l'uso dei fogli di lavoro dell'1-2-3. Contiene anche uno worksheet di tipo contabile, uno per il calcolo delle rate di mutuo, uno per la gestione delle mailing list e altro. Richiede 1-2-3.

☐ **592 TSHELL** Crea un ambiente di lavoro efficiente per operare sotto DOS. Manuale d'uso, messaggi di aiuto su schermo, note sulla installazione e l'impiego.

☐ **608 AUTOMENU** Per richiamare da menù i programmi, i file batch e i comandi DOS. Si installa una volta e serve sempre.

☐ **684 PAGEONE** Programma per l'elaborazione e la gestione di documenti di medie dimensioni. Crea un file grande quanto una pagina in formato lettera, con prestazioni che mancano o sono di difficile uso nei normali Word Processor. Ampia documentazione, anche in linea.

☐ **694 SLEUTH** Improvvisatevi investigatori e scoprite il colpevole di un assassinio tra sei individui sospetti. La trama cambia ogni volta. Anche monocromatico.

☐ **697-698-699 THE FRONT OFFICE** Gestione delle vendite, degli ordini, analisi del profitto e altro. Progettato in maniera specifica per le vendite dirette, ma facilmente adattabile ad altri tipi di business. Richiede disco rigido.

☐ **718 LQ PRINTER UTILITY** Fantastico programma che vi mette a disposizione molti font per Epson e altre stampanti: Courier, Greek, Helvetica, Palatino, Sans Serif ecc.

☐ **722 COMPOSER** Editor musicale su tre ottave. Contiene anche un programma per rendere accessibili da Turbo Pascal i pezzi creati tramite Composer.

☐ **723 SUPER PINBALL** Grande raccolta di 5 diversi giochi del Flipper. Un menù consente di saltare dall'uno all'altro senza dover passare dal DOS.

☐ **734 EXTENDED DOS** L'ultima fatica di Jim Button, noto per i suoi Pc-File, Pc-Type e Pc-Calc. Aggiunge potenza e flessibilità al DOS. Molto ben documentato, anche con aiuti in linea.

☐ **763 FINGER PAINT** Programma completo di disegno. Funziona sia con la scheda CGA che con la Hercules.

### I Best Seller di sempre

☐ **5-730 PCFILE +** Il notissimo Database in versione potenziata.

☐ **10 CHASM** Compilatore Assembler con tutorial.

☐ **69 DESIGNER** Editor per la grafica.

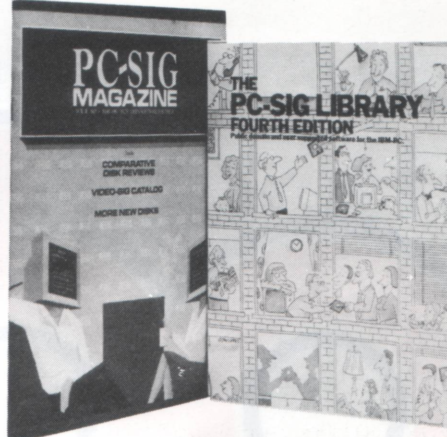
☐ **82 BATCH FILE UTILITIES** Indispensabile per sfruttare al meglio le possibilità dei files Batch del DOS.

☐ **106 DISKCAT** Per catalogare i vostri dischetti. 41K di documentazione.

- [ ] **120 PC-CHESS** Programma di scacchi.
- [ ] **254 PC DOS HELP**
- [ ] **273 BEST UTILITIES**
- [ ] **274 BEST GAMES**
- [ ] **293 ARCADE GAMES**
- [ ] **309 ASSEMBLY PROGRAMS** Grande raccolta di programmi esemplificativi che svelano i segreti del Macro Assembler IBM. Fanno anche risparmiare tempo a chi già conosce questo linguaggio di programmazione.
- [ ] **347 PC-FOIL** Editor che permette di combinare in maniera semplice il testo con diagrammi non complessi.
- [ ] **351 TURBO TOOLS** Tutto ciò che serve a chi programma in Turbo Pascal.
- [ ] **405 DESKMATES** Agenda, calcolatrice, rubrica telefonica, segretaria personale.
- [ ] **478 HARD DISK UTILITIES**

## La Membership in Regalo

**La nostra proposta di Associazione ha avuto un successo clamoroso e pertanto abbiamo deciso di rinnovarla. Oggi acquistando il volume The PC-SIG Library più 5 dischi a scelta ricevete in regalo la Membership per un anno. Per sole 115.000 lire (addirittura 14.000 lire meno di ieri) diventate anche Soci e vi assicurate la Newsletter bimestrale, nonché il diritto ad uno sconto (da 1.500 a 6.000 lire) sull'acquisto di altri dischi.**
***Strettamente riservato ai vecchi Soci: con l'acquisto di 5 dischi a prezzo Associati avrete in omaggio la nuova edizione di The PC-SIG Library.***
**Compilate subito il tagliando e speditelo oggi stesso. Non dovete obbligatoriamente scegliere tra i titoli proposti qui: potete esaminare il catalogo a casa vostra e decidere con tutta calma.**




***Oltre 100.000 copie vendute nel mondo.***
***4° Edizione rinnovata e ampliata***

---

**ULTIMOBYTE** S.r.l. - Via Aldo Manuzio, 15 - 20124 Milano
**Ordini telefonici: 02/65.97.693**
*Tutti i prezzi esposti comprendono l'IVA. Aggiungere all'importo di ogni ordine il contributo fisso di L. 4.000 per spese di spedizione.*

- [ ] **SI** aderisco alla vostra proposta di Membership
  - [ ] Inviatemi a L. 115.000 "The PC-SIG Library", la Newsletter e 5 dischetti. Scelgo: ______ cod. 1 ______ cod. 2 ______ cod. 3 ______ cod. 4 ______ cod. 5
  - [ ] A semplice richiesta e senza ulteriori spese mi invierete i rimanenti ______ dischetti che mi spettano.
- [ ] **NO** non desidero diventare Socio. Rinuncio alla Newsletter e allo sconto. Inviatemi comunque ________________________________

Totale da pagare L. ____________ + L. 4.000 = L. ____________

| ASSOCIATO | ABBONAMENTO ULTIMOBYTE |
|---|---|
| Solo se siete già Soci barrate questa casella. Ricordate che ordinando 5 dischi avete diritto al nuovo catalogo in omaggio. | Per abbonarvi a Ultimobyte barrate questa casella. 11 numeri a L. 126.000 con un risparmio di 28.000 lire sul prezzo di copertina. |

- [ ] Allego assegno/vaglia postale
- [ ] Pagherò al postino in contrassegno

NOME ____________________ COGNOME ____________________
VIA ____________________ CITTÀ ____________________ (______)
CAP ____________ P.IVA/Cod. Fisc. ____________________
(solo se si desidera fattura)